International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 39-45

http://www. irphouse.com

Approach for Image Security by Merging LSB and IDEA Algorthim

Abhishek Kumar Kashyap

Department of Computer Science and Engineering
Galgotias University Greater Noida, Uttar Pradesh, India
ABHISHEKGLB19@gmail.com

1 Introduction:

Steganography is the embedding of messages within an innocuous cover work in a way which can not be detected [1] by anyone without access to the appropriate steganographic key. Wikipedia calls steganography, incorrectly, a form of "security through obscurity". This is not true as a correctly designed, key-based system will resist attackers that know the details of the algorithm but not the key. Steganalysis is the study of attacking such systems, analagous to cryptanalysis of cryptographic systems.

2 Method:

2.1 Steganography Techniques:

These techniques have in common the goal of embedding data in perceptually indistinguishable parts of an image. [1]

2.1.1 EzStego:

EzStego embeds data in GIF images, by altering the colors of pixels. To do this imperceptibly, it sorts the image's palette to minimize the perceptual distance between consecutive colors. This is achieved by finding the shortest-path between the palette colors within the RGB color space cube. Then, the message is embedded by altering pixels, in order, so that the least significant bits of the pixels' indexes into the sorted palette are the message bits. [1]

2.1.2 Steganos:

Steganos embeds data in the least significant bits of image files. It replaces this data completely in the cover image, regardless of message length. [2]

2.1.3 JSTEG:

JSTEG embeds each message bit into more than one bit of the cover image, to reduce the detectible effects of the embedding. This is achieved through transforming the image by dividing it into blocks and applying the discrete cosine transform, and then altering coefficients and transforming back. This results to each message bit affecting an entire block in the cover image, making it harder to detect the changes. [2]

2.1.4 Encoding Secret Messages in Images:

Steganography, this field will continue to grow at a very rapid pace. 8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color will be harder to detect after the image has been encoded with the secret message [5]. 24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded. The other benefit is that a much larger amount of hidden data can be encoded into a 24-bit digital image as opposed to an 8-bit digital image. The one major drawback to 24-bit digital images is their large size (usually in MB) makes them more suspect than the much smaller 8-bit digital images (usually in KB) when sent over an open system such as the Internet. [5]

3 Research Objective:

Our concept deals with image steganography. Various steganographic algorithms like Least Significant Bit (LSB) algorithm, Jsteg and F5 algorithms, out of these we are using LSB algorithm. First I will review the techniques which are used in the stegengrophy and after this I will concentrate on one technique for stegengraphy

The aim of the my research paper is to hide the data in the form of text, audio, video, digital images using least significant steganographic algorithm and also with the help og IDEA algorthim to design new approach for image security to send the stego file to the destination where the retrieving of the secret data is done.

3.1 To design new approach for image security:

In this I design a new approach for security.

3.2 To combine IDEA and LSB for image protection:

In this I am combining IDEA and LSB for better image security. Now I am explain IDEA and LSB algothim.

3.2.1 The IDEA Algorthim:

International Data Encryption Algorithm (IDEA) is a block cipher designed by Xuejia Lai and James L. Massey of ETH-Zürich and was first described in 1991. It is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). IDEA was used as the symmetric cipher in early versions of the Pretty Good Privacy cryptosystem. [6]

The IDEA encryption algorithm:

- provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
- is fully specified and easily understood
- is available to everybody
- is suitable for use in a wide range of applications
- can be economically implemented in electronic components (VLSI Chip)
- can be used efficiently
- may be exported world wide
- is patent protected to prevent fraud and piracy.

The 64-bit plaintext block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

Encryption:

The functional representation of the encryption process is shown in Figure 1. The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail.

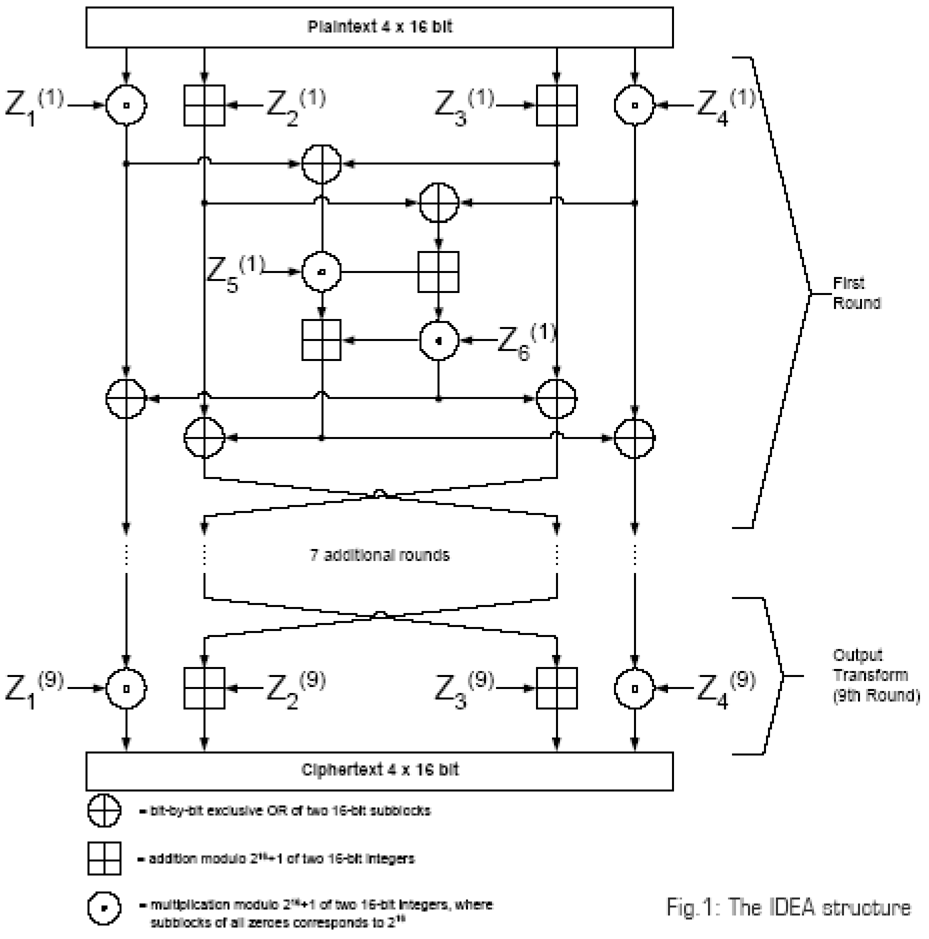
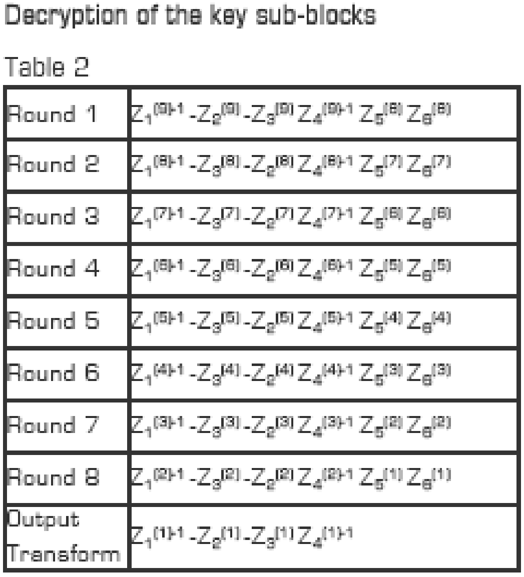

Plaintext 4 x 16 bit
$Z_1^{(1)}$
$Z_2^{(1)}$
$Z_3^{(1)}$
$Z_4^{(1)}$
$Z_5^{(1)}$
$Z_6^{(1)}$
First Round
7 additional rounds
$Z_1^{(9)}$
$Z_2^{(9)}$
$Z_3^{(9)}$
$Z_4^{(9)}$
Output Transform (9th Round)
Ciphertext 4 x 16 bit
= bit-by-bit exclusive OR of two 16-bit subblocks
= addition modulo 2¹⁶+1 of two 16-bit integers
= multiplication modulo 2¹⁶+1 of two 16-bit integers, where subblocks of all zeroes corresponds to 2¹⁶

Fig.1: The IDEA structure

In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$. The results are then processed further as shown in Figure 1, whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo $2^{16} + 1$ to form the resulting four 16-bit ciphertext blocks.

Decryption:



Decryption of the key sub-blocks

Table 2

Round 1	$Z_1^{(9)-1}$ $-Z_2^{(9)}$ $-Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
Round 2	$Z_1^{(8)-1}$ $-Z_3^{(8)}$ $-Z_2^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
Round 3	$Z_1^{(7)-1}$ $-Z_3^{(7)}$ $-Z_2^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
Round 4	$Z_1^{(6)-1}$ $-Z_3^{(6)}$ $-Z_2^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
Round 5	$Z_1^{(5)-1}$ $-Z_3^{(5)}$ $-Z_2^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
Round 6	$Z_1^{(4)-1}$ $-Z_3^{(4)}$ $-Z_2^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
Round 7	$Z_1^{(3)-1}$ $-Z_3^{(3)}$ $-Z_2^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
Round 8	$Z_1^{(2)-1}$ $-Z_3^{(2)}$ $-Z_2^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Output Transform	$Z_1^{(1)-1}$ $-Z_2^{(1)}$ $-Z_3^{(1)}$ $Z_4^{(1)-1}$

The computational process used for decryption of the ciphertext is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated.

More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process as shown in Table 2.

Literature/Research Survey:

Year	Paper Author	Title	Abstract	Keyword	Publication
2009	M.Sitaram Prasad	A Novel Information Hiding Techniques For Security By Using Image Steganography [1]	In this paper a novel method is proposed to provide more security for the key information with the combination of image compression and data encryption method. This method requires less memory space and fast transmission rate because of image compression technique is applied.	Compression, Steganography, Digital watermarking, public key Encrption, Decryption, Fingerprinting	JATIT

2011	Amitava Nag	Novel Techniques for image steganography based on dwt and Huffman encoding [2]	Image steganography is the art of hiding information into a cover image. This paper presents a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain.	Steganography, Frequency Domain, dwt, Huffman Coding, Information Hiding	IJCSS VOLUME (4)
2012	Abikoye Oluwakemi C.	Effystem Data Hiding System Using Cryptographyand Steganography [3]	In this paper, a data hiding system that is based on audio steganography and cryptography is proposed to secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file.	Electronic exchange, Cryptography, Steganography, Least Significant Bit, Algorithm	IJAIS Vol (4)
2012	Mr.Vias Tyagi	Data hiding In Image Using Least Significant Bit With Cryptography [4]	This paper discussed a technique used on the LSB ans a new encryption algorthim.	Steganography, lsb, Encryption, Decryption, Data Security	IJARCSSE Vol (2)
2012	Joham GroBschadl	Efficent Java Implentation Of Elliptical Curve Cryptography For J2me Enabled Mobile Devices [5]	In this paper, we present an optimized java implementation of ec scaler multiplication.	Steganography, JVM, J2ME	SPRINGER
2013	Juan José Roque,	SLSB: Improving the Steganographic Algorthim Lsb [6]	In this paper, we implement slsb technique over the lsb technique.	Security, Steganography, Least Significant Bit.	IEEE

2013	Dr. Mazen M Al Hadidi	Data Hiding Using Least Significant Bit Approch [7]	we implemented the Least Significant Bit technique to hide data such as doc file into image of JPEG format and send the image from a source to a destination through a wireless network.	Security, Hiding, Sinternet, Least significant Bit.	IEEE
2013	Jaspal Kaur Saini	A Hybrid Approach for Image Security by Combining Encryption and Steganography. [8]	This presents the hybrid approach for image security that combines both encryption and steganography. First the image is encrypted using proposed new version of AES algorithm, which is then hided into cover image using the steganography concept.	Information Security, Cryptography, Steganography, Advance Encryption Standard (AES), Modified Advance Encryption Standard (MAES), Image Encryption, Image Steganography.	IEEE

References:

[1] M.Sitaram Prasad, S.Naganjaneyulu, CH.Gopi Krishna, C.Nagaraju (A Novel Information Hiding Technology Technique for security By using Image steganography) (JATIT).

[2] Amitva Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar (A Novel Techinque for Image Steganography Based On DWTand Huffman Encoding) (IJCSS), VOL (4).

[3] Abikoye Oluwakemi C., Adewole Kayode S., Oladipupo Ayotunde J. (Efficent Dta Hiding System Using cryptography and Stegnography) (IJAIS) VOL (4).

[4] Mr.Vikas Tyagi (Data Hiding In Image using Least Significant bit With Cryptography) (IJARCSSE), VOL (4).

[5] Johann GroBschadl, Dan Page, Stefan Tillich, (Efficent Java Implementation Of Elliptic Curve Cryptography for J2ME-Enabled Mobile Devices (IEEE).

[6] Juan Jose Roque, Jesus Maria Minguet, (SLSB: Improving the Steganographic Algotithm LSB) (IEEE).

[7] Dr. Mazen M Al Hadidi, Dr.Yasir Khalil Ibrahim, (Data Hiding Using Least Significant Bit Approch) (IEEE).

[8] Jaspal Kaur Saini, Harsh K Verma, (A Hybrid Approach for Image Security by Combining Encryption and Steganography) (IEEE)